REMARKS

The Examiner is thanked for the thorough examination of this application. The non-FINAL Office Action after RCE, however, continued to reject all examined claims. In response, Applicant submits the foregoing amendments and the following remarks. In this regard, independent claim 1 has been amended to further define the "standard file set and parallel file set," and claims 14 and 23 have been amended for consistency with claim 1.

The Office Action rejected claims 1-2, 5-13, 31 and 36 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Yamada et al. (U.S. Patent 6,490,683) and further in view of Ohgake (U.S. Pub. 2001/0044887) and Sasaki et al. (U.S. Pub. 7,024,534). Further, Claims 14-28 and 30 stand rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Yamada et al., Ohgake and Sasaki, and further in view of Ando et al. (U.S. Patent 6,907,187). Further, Claims 33-35 and 37 are rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Yamada et al., Ohgake, and Sasaki, and further in view of Serpa (U.S. Patent 6,954,862). Claim 29 is rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Yamada, Ohgake, Sasaki, and Ando, and further in view of Serpa.

According to the current amendment, a "standard file system" in the standard file set has been included, wherein the standard file system has a dummy directory tree pointing to dummy data. In this regard, reference is made to page 6, lines 29-33 of the present application, which states: "*The directory tree of dummy data is stored in the UDF directory structure in UDF file system **822**. Wherein, the directory tree includes root directory record **802**, directory records **803** and file records **804**. Although we already*

knew that file records contains data addresses that point to some dummy data content 805". Accordingly, the amendment adds no new matter to the application, and more clearly defines over the cited art.

In addition, it is featured that the standard file system defines the next available address as the start of the secret file set descriptor, which is described in page 7, lines 21-24 of the present application, which states: "*The UDF file system will now read the dummy directory tree and find out where the tree ends in order to define the next available address as the start of secret file set descriptor* ***810*** *in the preferred embodiment of the present invention* ***S514****. The secret file set descriptor* ***810*** *belongs to the non-standard directory files and records in the UDF system.*" Also see the operation 302 in FIG. 3 in sequence.

Further still, the amended claim 1 defines that parallel file set includes the secret file set descriptor and the real directory tree pointing to the real data, which is described in page 5, lines 8-13 of the present application, which states: "*The secret file set descriptor* ***310*** *stores a preset address that points to a root directory record of a real directory tree in UDF system. This real directory tree is stored in a secret UDF directory structure* ***312*** *and containing root directory record, directory records and file records. Wherein the file records hold some data addresses that point to the actual data content of the optical disc inside a secret files* ***314****.*"

As claim 1 now clearly defines, the method for encoding a confidential optical disc with a burner includes a first step of receiving a signal for creating the confidential optical disc to switch a burner into a burning mode. Next, the method sets a data-accessing password for future verification, wherein the data-accessing password is

placed to a secret file set descriptor and allocated on any unoccupied space of an optical disc; and wherein the secret file set descriptor is a non-standard file and stores a preset address pointing to a root directory record of a real directory tree. Further, the step of selecting one of data sources for public viewing and confidential viewing data to be burned on the disc, receiving a start burn signal to begin a data encoding process, and creating a temporary file system as a buffer are included. Furthermore, the temporary file system provides two stages, that is:

(1) creating a standard file set comprising a standard file system including a dummy directory tree pointing to dummy data, wherein the standard file system defines the next available address as the start of the secret file set descriptor; and

(2) creating a parallel file set comprising the secret file set descriptor and the real directory tree pointing to with real data.

Finally, the method burns the buffer to the optical disc to produce the confidential optical disc.

Applicant submits that these features clearly define claim 1 over the cited references. In addition, Applicant submits the following distinguishing remarks.

Yamada (US 6,490,683)

The previous Office Action admitted that Yamada fails to disclose the step of "selecting one of data sources for public viewing and confidential viewing data to be burned on the disc." In this regard, the cited paragraph, Lines 1-20, col. 8, does not disclose public viewing nor confidential viewing data.

Yamada also fails to disclose the claimed feature of: "*wherein the data-accessing password is placed to a secret file set descriptor and allocated on any unoccupied space of an optical disc, and* ***wherein the secret file set descriptor is a non-standard file and stores a preset address pointing to a root directory record of a real directory tree.***"

Sasaki (US 7,024,534)

Sasaki does not disclose "***the data-accessing password is placed to a secret file set descriptor*** and ***allocated on any unoccupied space of an optical disc***" of claims 1 and 31.

The claimed secret file set descriptor has a unique or non-standard structure at an unknown location allocated on any unoccupied space of an optical disc so that general optical disc player/reader cannot access the secret file set descriptor.

In contrast, Sasaki describes "where" is an unallocated location such as "*In a space management structure area 421 of the latest file structure area 431, the space management structure is recorded. The space management structure includes the unallocated space entry 453."* and Fig. 6 shows *""unallocated space entry 652*".

For example, as described by Sasaki, *see* col. 14, line 64, "*An unallocated space entry 155, which is a space management structure, includes a descriptor tag 185 indicating that the entry is an unallocated space entry, and positional information of at least one unallocated area existing in the volume space (in the example shown in FIG. 1, positional information 186 of an unallocated area #1, positional information 187 of an unallocated area #2, positional information 188 of an unallocated area #3, and positional*

information 189 of an unallocated area #4)." Sasaki, however, provides no description of "what" is stored in the unoccupied space. On the other hand, claim 1 clearly defines "***data-accessing password is placed to a secret file set descriptor and allocated on any unoccupied space of an optical disc***". Claim 1, therefore, clearly defines over the relevant teachings of Sasaki.

The amended claim 1 further describes the location of "secret file set descriptor" as "comprising a standard file system including a dummy directory tree pointing to dummy data, wherein the standard file system defines the next available address as the start of the secret file set descriptor;" and "creating a parallel file set comprising the secret file set descriptor and the real directory tree pointing to real data." In other words, the secrete file set descriptor is placed at an unoccupied space when burning, and its start address is defined by the standard file system, which defines the next available address as the start of the secret file set descriptor. (See page 7, lines 22-24 of the present application, which states: "*The UDF file system will now read the dummy directory tree and find out where the tree ends in order to define the next available address as the start of secret file set descriptor 810 in the preferred embodiment of the present invention S514. The secret file set descriptor 810 belongs to the non-standard directory files and records in the UDF system.*")

Nowhere the cited paragraphs does Sasaki disclose the "secrete file set descriptor" and the "location" of the secrete file set descriptor, as defined in claims 1 and 31. Indeed, referring to col. 11, lines 60-63, Sasaki describes that the basic file structure area of a latest file structure area 431, the basic file structure is recorded.

The basic file structure includes a file set descriptor 450, a root directory 451, and a file entry (root directory) 452.

This is essentially the same as previous prior art Geeslin, which described that the file set descriptor and root directory are clearly defined in the DVD standard. This is known to the public and thus to persons skilled in the art, and they are called "standard" file set descriptor, which is fundamentally different from the "secrete file set descriptor" of the presently claimed embodiments. As expressly defined in amended claim 1, the secret file set descriptor is pointed by the address stored in the sequence (*see* operation 302 in FIG. 3) and can *only be found by the optical disc player/reader* using the method of the present application. In particular, the secret file set descriptor stores a preset address that points to a root directory record of a real directory tree in the UDF system.

Referring to lines 1-12, col.12 of Sasaki, Sasaki describes that the VAT contains the correlation between virtual and logical address, and the purpose of VAT and secrete file set descriptor is different. Sasaki describes the purpose of resolving the problem that "the latest data is recorded by rewriting data in an identical area." In col. 15 lines 45-53, Sasaki describes: "By registering the **unallocated areas in the unallocated space entry 155** in the above-described order and recording the data in the unallocated areas in the order of registration in the unallocated space entry 155, data can be recorded while moving the latest file structure area on the optical disc. As a result, **concentration of data rewrite in a specific area can be avoided**, and thus occurrence of defects and data destruction can be prevented." Thus, the paragraph of col. 12, lines 1-12 is simply unrelated to the invention defined by claim 1.

The logical address represents a new recording position and it is updated into VAT. In col. 14, lines 18-31, Sasaki describes: "By updating a logical address in the VAT 653 describing the correspondence between the virtual addresses and the logical addresses, the new recording position can be accessed using the same virtual address." Thus, this paragraph only relevantly describes "how to locate" an unallocated location and "how to update" the logical address.

As expressly defined in amended claim 1, the secret file set descriptor is pointed by the address stored in the sequence (*see* operation 302 in FIG. 3) and can *only be found by the optical disc player/reader* using the method of the present application. In particular, the secret file set descriptor stores a preset address that points to a root directory record of a real directory tree in the UDF system.

The address of secret file set descriptor is located at a next available address followed by dummy directory tree. The location of real or dummy address is NOT updated.

Again, referring to col. 14, lines 18-31, Sasaki describes that "the system control section 201 reads a file entry (root directory) 154 and a root directory 153 from a file set descriptor 152 while **converting** the virtual address into a logical address using the VAT." The dummy or real address is not equivalent, so they do not covert to each other. Consequently, not only does Sasaki fail to disclose the invention defined by claim 1, Sasaki actually teaches away from claim 1.

Ohgake (U.S. Pub. 2001/0044887)

For reasons similar to those described above and in Applicant's previous response, Ohgake does not disclose "secret file set descriptor" nor the location of "secrete file set descriptor".

Ando (U.S. Patent 6,907,187)

Compared to Ando, the dummy data or public viewing data of claims 1, 14, 23, 30, and 31 can be read by anyone and as such is clearly different from the "dummy pack 89" of U.S. Patent Application No. 6,907,187 (Ando), wherein the dummy pack 89 is used for allowing users to edit the contents of the recording after having recorded the video title set VTS in Lines 16-23, col. 11 of Ando. Thus, Ando also teaches away from claim 1.

Simply stated, in view of the foregoing, independent claim 1 patently define over the cited art for at least the reasons that the cited art fails to disclose the features that are emphasized below in claim 1:

> 1. A method for encoding a confidential optical disc with a burner, the method comprising the steps of:
> receiving a signal for creating the confidential optical disc to switch a burner into a burning mode;
> setting a data-accessing password for future verification, wherein the data-accessing password is placed to a secret file set descriptor and allocated on any unoccupied space of an optical disc, wherein the secret file set descriptor is a non-standard file and stores a preset address pointing to a root directory record of a real directory tree;
> selecting one of data sources for public viewing and confidential viewing data to be burned on the disc;
> receiving a start burn signal to begin a data encoding process;
> ***creating a temporary file system as a buffer that includes two stages:***

creating a standard file set comprising a standard file system including a dummy directory tree pointing to dummy data, wherein the standard file system defines the next available address as the start of the secret file set descriptor, and
creating a parallel file set comprising the secret file set descriptor and the real directory tree pointing to real data; and
burning the buffer to the optical disc to produce the confidential optical disc.

For at least the foregoing reasons, claim 1 patently defines over the cited art. Insofar as claims 2 and 5-30 depend from claim 1, the rejections of these claims should be withdrawn for the same reasons.

Claim 31.

With regard to independent claim 31, as amended herein, this claim recites:

31. A method for reading and decoding a confidential optical disc produced by claim 1, the method comprising the steps of:
a player reading optical disc data;
receiving a view confidential data command signal;
requesting entry of a data-accessing password;
comparing the entered password with a data-accessing password placed in a secret file set descriptor allocated on any unoccupied space of an optical disc, wherein the secret file set descriptor is a non-standard file and stores a preset address pointing to a root directory record of a real directory tree;
if the entered password is correct, playing or reading real data, wherein the real data of the optical disc is pointed by the preset address; and
ending the playing/reading session.

(*Emphasis added*). Claim 31 patently defines over the cited art for at least the reason that the cited art fails to disclose the features emphasized above.

Claim 31 further defines claim 1 and defines a step of reading and decoding the confidential optical disc. As set for above, nowhere the cited paragraphs does Sasaki disclose the "secrete file set descriptor" and the "location" of the secret file set descriptor, as defined in claims 1 and 31. In addition, Applicant submits that neither Yamada nor Sasaki, nor any proper combination of the two teaches how to read the confidential optical disc after the operations of claim 1 by using the "data-accessing password." For at least this additional reason, the Sasaki reference fails to teach the idea of "secret file set descriptor" allocated on the unoccupied space. Further still, the cited references to not suggest the use of the data-accessing password to determine the correction of password. For at least these additional reasons, the rejection of claim 31 should be withdrawn.

CONCLUSION

Applicant respectfully submits that all pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephone conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (770) 933-9500.

No fee is believed to be due in connection with this amendment and response to Office Action. If, however, any fee is believed to be due, you are hereby authorized to charge any such fee to deposit account No. 20-0778.

Respectfully submitted,

/Daniel R. McClure/

Daniel R. McClure
Reg. No. 38,962

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.
600 Galleria Parkway SE
Suite 1500
Atlanta, Georgia 30339
(770) 933-9500